AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

A BLACK ZTE CELL PHONE (currently in an envelope labeled with an evidence receipt citing the Lemicy case) securely stored at the United States Attorney's Office, 111 S. 10th Street, St. Louis, Missouri 63102, Eastern District of Missouri.

Case No. 4:22-MJ-7241-SPM

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Michael Spreck, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

18 U.S.C. §§ 2251(a) and 2252A, using a minor to produce a visual depiction of minor engaged in sexually explicit conduct and possession of child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Applicant's signature

Michael Spreck, TFO

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures 4.1 and 41.

Date: 08/25/2022

Judge's signature

City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: Colleen C. Lang

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF A BLACK ZTE CELL PHONE (currently in an envelope labeled with an evidence receipt citing the Lemicy case) securely stored at the United States Attorney's Office, 111 S. 10th Street, St. Louis, Missouri 63102, Eastern District of Missouri.	No. 4:22-MJ-7241-SPM SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Michael Spreck, a Detective with the Saint Louis Metropolitan Police Department and Task Force Officer (TFO) with the FBI, being duly sworn, depose and state the following:

INTRODUCTION AND OFFICER BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the cell phone listed in Attachment A, for the things described in Attachment B.

2. I have been employed with the Saint Louis Metropolitan Police Department (SLMPD) since March 1995. I have investigated federal criminal statutes involving the sexual exploitation of children under Chapter 110 of Title 18, United States Code Section 2251 and 2252A. As a FBI TFO and as a SLMPD detective, I have acquired experience in these matters through specialized training, everyday exposure/work related to these types of investigations, as well as information imparted to me by other law enforcement officers involved in similar investigations.

3. This affidavit is submitted in support of an application for a search warrant to a ZTE cell phone, further described in Attachment A for evidence described in Attachment B, that

involve violations of 18 U.S.C. §§ 2251(a) and 2252A, using a minor to produce a visual depiction of minor engaged in sexually explicit conduct and possession of child pornography.

4. The statements contained in this Affidavit are based on my investigation, and my experience, training, and background. I have not included every fact known to me concerning this investigation, but have set forth only those facts necessary to establish probable cause to believe that evidence of the crimes referenced herein will be found on the item to be searched.

PROPERTY TO BE SEARCHED

5. The property to be searched is a ZTE cell phone, black in color, currently stored within an envelope labeled with an evidence receipt citing the Lemicy case information, (hereafter "Subject Device"), which was seized on August 12, 2022. Subject Device is currently securely stored and located at the United States Attorney's Office, 111 S. 10th Street, St. Louis, Missouri, within the Eastern District of Missouri, and as detailed in Attachment A.

DEFINITIONS

6. The following terms have the indicated meaning in this affidavit:

a) The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable handheld calculator, or other similar device. 18 USC § 1030(e).

b) The term "minor" means any individual under the age of 18 years. 18 USC § 2256(1).

c) Sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the anus, genitals, or pubic area of any person. 18 USC § 2256(2)(A).

d) Visual depiction includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 USC § 2256(5).

e) Child pornography means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 USC § 2256(8)(A) or (C).

f) Identifiable minor means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 USC § 2256(9).

g) "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit

electronic, magnetic, or similar computer impulses or data, including for example, tablets, digital music devices, portable electronic game systems, electronic game counsels and wireless telephones. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h) "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i) "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j) "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code

may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k) The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

l) Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

m) "Wireless telephone or mobile telephone, smartphone or cellular telephone" as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional

"land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

PROBABLE CAUSE

7. In July of 2019, the St. Louis Metropolitan Police Department (SLMPD) began an investigation into concerns that several young females were sexually assaulted by a caregiver, identified as Anthony Lemicy (hereafter "LEMICY"). Concern also arose that LEMICY captured illicit video(s) of the victims.

8. The investigation included the seizure of one of LEMICY'S electronic devices, a LG Smartphone from his apartment on July 25, 2019. LEMICY gave written and verbal consented to SLMPD Det. Todd Hefele to search that LG Smartphone device. Subsequently, on August 2, 2019, a state-level search warrant was granted and executed on the device.

9. Initial attempts to unlock and examine the LG Smartphone were met with negative results because the device was password protected, and the password willingly provided by LEMICY was incorrect. A forensic examination of a memory card, contained within the

smartphone, revealed digital evidence (images and video) in support of the case against LEMICY. Subsequently, a Federal Grand Jury indicted LEMICY for one count of Sexual Exploitation of a Minor based on two videos of produced child pornography located on the SD card of the LG smartphone. On or about September 1, 2020, law enforcement made another attempt to extract data from LEMICY's LG Smartphone using software provided by the office of the United States Secret Service. That attempt successfully bypassed the user lock code. With the user lock code bypassed, the LG Smartphone digital contents were accessed.

10. While examining the digital contents pursuant to the search warrant, Det. Hefele viewed numerous videos on the LG Smartphone that, according to metadata associated with the files, had been produced with said device. At least three (3) video files were located on LEMICY's LG Smartphone depicted an adult male and a prepubescent female together in a bedroom. In one video, a penis, proportionally consistent with an adult male, is repeatedly placed on the child, specifically on the area around the child's vagina. At times, the male holds/guides his penis with his hand, particularly when he pushes his penis into the child's genitalia. In another video from the LG Smartphone, the adult penis is attempting the penetrate the child's anus. In a third video, a voice – that sounds much like LEMICY's voice – is talking to the child while the child's unclothed genitals are being recorded by LEMICY's LG Smartphone. Law enforcement determined that the child in these (3) videos was seven (7) year old, "LR." This conduct was charged on April 28, 2021, in a superseding indictment against LEMICY, adding three more counts of Sexual Exploitation of a Minor. See case number: 4:19CR0770HEA, *United States v. Anthony Lemicy*.

11. Law enforcement located the children depicted in the videos located on the LG Smartphone. The children, who alleged they were victimized by LEMICY, were interviewed by

law enforcement and the Children's Advocacy Center about what happened at LEMICY's home in July of 2019. Two of the children have even testified in a state court case about being molested by LEMICY. In some of their statements, the children describe being recorded or photographed by LEMICY. Specifically, at age eleven (11) "MR," a female child, told police that LEMICY had taken photographs of her and another minor female in the shower. In the state court trial MR testified she remembered LEMICY taking video or pictures of her in the shower. MR described that she was in the shower and saw LEMICY with the phone. *Missouri v. Lemicy*, 1922-CR02475, State Court Trial Transcript, November 2, 2020, ("State Court Tr.") at 110-111, 124.

12. At age ten (10), female child, "RR" testified in the state court case and stated that LEMICY "was taking pictures of us when we was in the shower, me and "MR" and "LR." "I was taking a shower and I was looking for my towel and the soap. So I bend over to get my soap and I saw him in a bathrobe taking pictures with his phone and we saw it on his phone." State Court Tr. at 71-72. Later in trial during cross examination "RR" was asked again if she saw pictures of herself in the shower on LEMICY's phone and she confirmed that. She also confirmed that MR and LR were also present. State Court Tr. at 84.

13. Law enforcement has located two shower videos on LEMICY's LG Smartphone. These depict minor victims, "MR" and "KC." The videos that "RR" testified about at trial have not been located.

14. On the morning of August 12, 2022, United States Attorney's Office Investigator Donya Jackson responded to the home of minor victim, eleven (11) year-old "KC." Investigator Jackson met with "KC's" mother, "TC," about an upcoming trial involving LEMICY. Later that morning, TC texted Investigator Jackson the following message: "i totally freaking forgot," "we

have his phone too" "Ive been trying to get in it for years maybe you can." Investigator Jackson responded back to the home of TC. TC and KC met Investigator Jackson outside of their home and handed Investigator Jackson a black ZTE cell phone (Subject Device). The Subject Device was in a powered down condition. TC signed a consent form allowing Investigator Jackson to seize and search the Subject Device.

15. TC further stated to Investigator Jackson that on the day that the police came to LEMICY's residence she and her daughter, KC, went into LEMICY's apartment after everyone had left so KC could use the restroom. Investigator Jackson knew that TC was referring to LEMICY's arrest in July of 2019. KC stated to Investigator Jackson that KC saw the Subject Device on a counter in LEMICY's apartment. It had no case on it so she thought it may have been her friend's phone that had been missing. KC took it upon leaving the apartment. TC stated that she attempted to charge Subject Device when they got home. Once the Subject Device was turned on both TC and KC observed LEMICY's face on the screen of the Subject Device. TC stated that the Subject Device asked for a login and they were unable to unlock Subject Device. TC stated that since July of 2019, the Subject Device has been stored in her closet. KC was asked if she knew if LEMICY used Subject Device. KC responded that she recognized the cell phone as the one LEMICY used when she stayed with him and that she would call her mother from this cell phone (Subject Device). KC stated she remembered he would walk around with Subject Device and remembers it in his hands. TC stated she remembered LEMICY having at least three (3) cell phones.

16. Further, on August 23, 2022, during a pre-trial meeting with mother of victim, LR (see earlier paragraph number ten), LR's mother stated to Investigator Jackson that LEMICY had three (3) cell phones in his possession back in 2019. She had seen him with cell phones and was

acquainted with LEMICY because she had dated LEMICY in the past.

17. Law enforcement has not been able to locate the child pornography images that victim "RR" described of her in the shower with two other children. The Subject Device was located in LEMICY's apartment and according to a witness was utilized by him. LEMICY is currently awaiting trial on charges of Production of Child Pornography – where it is alleged in Count One that LEMICY videotaped two minor children in a shower with a cell phone (the aforementioned LG Smartphone.)

18. Affiant knows that Subject Device is a smartphone, which has the ability to take photographs, videos, make phone calls, access internet, store large amount of data (even after being deleted) play music and more.

CONCLUSION

19. Your affiant seeks permission to search the contents of the above Subject Device, which is also detailed in Attachment A and is currently located at the United States Attorney's Office, within the Eastern District of Missouri, for evidence of crimes of possession, production or attempted production of child pornography 18 U.S.C. §§ 2251(a), and 2252A.

BACKGROUND ON COMPUTERS, CELL PHONES, AND CHILD PORNOGRAPHY

20. In my training and experience, I know that cellular phones (including smartphones), contain software and hardware that are the same, if not more sophisticated, than a typical home computer. The term "computer," "hard drive," and "computer media," as used in this affidavit, also refers to cellular phone or smartphones.

21. I also know that "smartphones" often allow for cloud-based storage, and many users back up their phones on their home computers. Information contained in a cell phone that is connected to a desktop, laptop computer, or the cloud, can easily transfer onto other media.

22. A computer's ability to store images in digital form makes a computer an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

23. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

24. Collectors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, iCloud, and Hotmail, and social media applications such as Kik and Snapchat among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer, even if the user is accessing the information on their cellular "smart phone." Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

25. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's

favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SEARCH METHODOLOGY TO BE EMPLOYED

26. The search procedure of electronic data contained in a smartphone, computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a) on-site triage of computer system(s) to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s);

b) examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c) searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law

enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d) surveying various file directories and the individual files they contain;

e) opening files in order to determine their contents;

f) scanning storage areas;

g) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

h) performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

I state under the penalty of perjury that the foregoing is true and correct.

MICHAEL SPRECK
Task Force Officer
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 25th day of August 2022.

HONORABLE SHIRLEY P. MENSAH
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The following devices and media, currently located at the United States Attorney's Office, 111 S. 10th St., St. Louis, Missouri, within the Eastern District of Missouri:

Black ZTE SMART PHONE (no other significant markings), currently located within an envelope labeled with an evidence receipt citing the Lemicy case information.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The following are to be seized from the devices and media listed in Attachment A: Evidence, instrumentalities and contraband concerning the violations of Title 18, United States Code, Sections 2251, and 2252A.

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(8)(A) or (C).

2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all notes, documents, records, correspondence, in any format and medium (including, but not limited to, email messages, chat logs, electronic messages, notes), emails, computer logs, and browser and internet history pertaining to the production, possession, receipt or distribution of child pornography (or attempt to do so) or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(8)(A) or (C).

4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of the electronic devices and media listed in Attachment A.

5. Documents and records regarding the ownership and/or possession of the electronic devices and media listed in Attachment A.